UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/764,527 | 01/27/2004 | Tetsuro Motoyama | 245419US2 | 8977 |

22850 7590 12/10/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| FEARER, MARK D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2443 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 12/10/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

| | | | |
|---|---|---|---|
| *Office Action Summary* | **Application No.**<br>10/764,527 | **Applicant(s)**<br>MOTOYAMA ET AL. | |
| | **Examiner**<br>MARK D. FEARER | **Art Unit**<br>2443 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 August 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5 and 7-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-20, and 21-26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

**1.** Applicant's Amendment filed 17 August 2009 is acknowledged.

**2.** Claims 1-3, 5, 7-11, 13-18, 20 and 22-26 have been amended.

**3.** Claims 1-5, 7-20, and 22-26 are pending in the present application.

**4.** This application is made FINAL.

### *Claim Rejections - 35 USC § 103*

**5.** The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

**6.** Claims 1-5, 7-20, and 21-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitchell et al. (US 20040117494 A1) in view of Nadeau et al. (US 7099947 B1) and in further view of Seto et al. (US 20050138191 A1).

Consider claims 1, 9 and 16. Mitchell et al. discloses a system and method of determining which, if any, communication protocols can be used to extract status information related to a network device, comprising: storing, in a device object associated with the network device, protocol specific information obtained from a digital repository for a plurality of communication protocols ((“More particularly, the service provider 110 stores (or has access to) available services or software applications 112, available communication filters 114, and available protocol elements 116. As will become clear, communication channels built within the clients 130, 150, 170 and used by client applications or service components 140, 154, 180 are formed generally by the combination of a single protocol element, such as element 116, that defines network protocols and one or more communication filters, such as a filter(s) 114 that define communication parameters (such as what security measures are to be taken and how to apply such measures). A provisioning agent 118 is provided on the service provider 110 to control which services 112, filters 114, and protocol elements 116 are made available which clients 130, 150, and 170. The provisioning agent 118 responds to discovery requests from the clients 130, 150, 170 and when appropriate transfers or provisions the services 112, filters 114, and protocol elements 116 to the clients 130, 150, 170. The filters 114 and protocol elements 116 may be provided by the content providers 104 or another third-party and typically are registered within the service provider 110 (such as in a filter and protocol element registry) and then announced or pushed (or otherwise made available) to the clients 130, 150, 170. Once the filter 114 and/or network protocol element 116 has been deployed to the client 130, 150, 170 the client 130, 150, 170 may begin to use the filters 114 and elements 116 in forming or reconfiguring service component communication channels, as explained below in detail. The service provider 110 may further, such as with the provisioning agent 118, maintain a database (not shown) with information about which filters 114 and which protocol elements 116 have been deployed to which clients 130, 150, 170.") paragraph 0023); selecting a communication protocol among a plurality of communication protocols (("The system 200 further includes a second service component 270 that includes a communications channel 272 built by the channel factory 212 of the communications manager 210. The communications channel 272 differs from the communication channel 232 of the first service 230 and as shown, includes an in channel 276 having a protocol element 278 and a channel filter 280 made up of three of the available channel filters 218 concatenated together to provide a suite of upper layer protocols. The communications channel 272 includes an out channel 284 with a protocol element 286 selected from the available protocol elements 216 but differing from the protocol element 278 of the in channel 276 and with a channel filter 288 again selected from the filters 218 to differ from the in channel filter 280. As can be appreciated, the combination of available filters to form channel filters may be quite large as well as the combination of such channel filters with lower layer protocols defined by the protocol elements. In this fashion, the communications manager 210 is able to support dynamic updating and reconfiguring of the communication channels 232, 252, 272 independently of the state or operation of the services 230, 250, 270.") paragraph 0032); obtaining, from a device object associated with the network device, information for accessing the network device using the selected communication protocol (("More particularly, the service provider 110 stores (or has access to) available services or software applications 112, available communication filters 114, and available protocol elements 116. As will become clear, communication channels built within the clients 130, 150, 170 and used by client applications or service components 140, 154, 180 are formed generally by the combination of a single protocol element, such as element 116, that defines network protocols and one or more communication filters, such as a filter(s) 114 that define communication parameters (such as what security measures are to be taken and how to apply such measures). A provisioning agent 118 is provided on the service provider 110 to control which services 112, filters 114, and protocol elements 116 are made available which clients 130, 150, and 170. The provisioning agent 118 responds to discovery requests from the clients 130, 150, 170 and when appropriate transfers or provisions the services 112, filters 114, and protocol elements 116 to the clients 130, 150, 170. The filters 114 and protocol elements 116 may be provided by the content providers 104 or another third-party and typically are registered within the service provider 110 (such as in a filter and protocol element registry) and then announced or pushed (or otherwise made available) to the clients 130, 150, 170. Once the filter 114 and/or network protocol element 116 has been deployed to the client 130, 150, 170 the client 130, 150, 170 may begin to use the filters 114 and elements 116 in forming or reconfiguring service component communication channels, as explained below in detail. The service provider 110 may further, such as with the provisioning agent 118, maintain a database (not shown) with information about which filters 114 and which protocol elements 116 have been deployed to which clients 130, 150, 170.") paragraph 0023); determining if the network device can be accessed using the selected communication protocol and the information for accessing the network device obtained from the device object (("Preferably, the communications manager 132 and components 140, 154 are built up on a standardized service framework to facilitate composing the service components 140, 154 from a minimal code set with no or little duplication. For example, but not as a limitation, the framework or architecture for the client 130, 150 computing system may be an OSGi (Open Services Gateway Initiative) component framework. hi this example, Java.TM. 2 Platform, Micro Edition (J2ME) is utilized and the clients 130, 150 can be configured using connected limited device configuration (CLDC) or connected device configuration (CDC). Typically, the decision point for using CLDC or CDC is the capability, memory, and size of the client 130, 150 with CLDC being appropriate for light weight devices such as those using 16-bit processors with less than 2 megabytes (MB) of memory and CDC being useful when devices used 32-bit processors and memory of 2 MB or greater. Hence, the mobile client 130 may be an in-vehicle system or telematics control unit and be built on a J2ME CLDC platform standardized per OSGi. The light mobile client 150 may be a 16-bit processor with less than 2 MB memory (such as a PDA, cellular phone, or other mobile computing device) built on a J2ME CDC platform standardized per OSGi.") paragraph 0026); and if the determining step determines that the network device can not be accessed using the selected communication protocol, removing, from the device object, the information for accessing the network device using the selected communication protocol (("At 430, a set of service components are installed (such as the set 320 of FIG. 3), which may follow a relatively standard installation of a component within a standardized framework (such as within an OSGi container). At 440, the communications manager, such as with a channel factory, builds communication channels for each service component by combining a protocol element with one or more filters. Alternatively, the channel may be built upon instantiation of the particular service to insure that any updates to the protocol elements and/or filters are included within the communications channel. The service then uses the channel for controlling communications within or outside the computing system. At 450, new protocol plug-ins and/or add-on filters are received and, at 460, the sets of available protocol elements and/or filters are updated by loading or storing the received items as available to the services (and this may include removing outdated filters or protocol elements from the set of available filters and protocol elements). At 470, the communications manager acts to dynamically reconfigure existing communications channels as needed for the running service components.") paragraph 0037); repeating the selecting, obtaining, determining, removing, and performing steps for each protocol of the plurality of communication protocols (("The system of claim 1, further including a provisioning manager for receiving additional ones of the communications filters and making the additional filters available to the communications manager for use in the building of the communication channels and wherein the communications manager reconfigures at least one of the built communications channels based on the additional filters by repeating the building to create a reconfigured communication channel.") Claim 7 ("The method of claim 9, further including after the providing of a set of channel filters, provisioning another one of the channel filters and after the communication channel making repeating the communication request receiving, the channel filters selecting, the combining, and the making, whereby the communication channel is dynamically reconfigured.") Claim 14).

However, Mitchell et al. does not explicitly teach a system or method wherein a determining step determines that the network device can be accessed using the selected communication protocol, performing further tests to determine whether the selected communication protocol can be used to extract the status information from the network device.

Nadeau et al. discloses a system and method wherein a determining step determines that the network device can be accessed using the selected communication protocol, performing further tests to determine whether the selected communication protocol can be used to extract the status information from the network device (("In the second sub-phase, starting at block 614, the VACM MIB Table and associated MIB Views are used for access control. Each PDU that is received in a request contains a context string, a protocol operation and information identifying one or more MIB variables over which the specified operation is to be executed. In block 614, the context string is extracted from the request, and in block 616 the securityName is extracted from the context string.") column 16 lines 29-36).

Mitchell et al. discloses a prior art method and system for dynamically reconfiguring pervasive device communication channels upon which the claimed invention can be seen as an improvement.

Nadeau et al. teaches a prior art comparable method and apparatus providing controlled access of requests from virtual private network devices to managed information objects using simple network management protocol.

Thus, the manner of enhancing a particular device (method and apparatus providing controlled access of requests from virtual private network devices to managed information objects using simple network management protocol) was made part of the ordinary capabilities of one skilled in the art based upon the teaching of such improvement in Nadeau et al. Accordingly, one of ordinary skill in the art would have been capable of applying this known improvement technique in the same manner to the prior art method and system for dynamically reconfiguring pervasive device communication channels of Mitchell et al. and the results would have been predictable to one of ordinary skill in the art, namely, one skilled in the art would have readily recognized a method and system for managing protocols used to obtain status information from a network device.

However, Mitchell et al., as modified by Nadeau et al., does not explicitly teach a system or method of obtaining, by a monitoring device, from a device object associated with a network device, the application layer protocol specific information for accessing the network device using a selected communication application layer protocol.

Seto et al. discloses a system and method of an adaptor supporting different protocols comprising a method of obtaining, by a monitoring device, from a device object associated with a network device, the application layer protocol specific information for accessing the network device using a selected communication application layer protocol.

[Seto et al., paragraph 0007 and Figure 2] An adaptor or multi-channel protocol controller enables a device coupled to the adaptor to communicate with one or more connected end devices according to a storage interconnect architecture, also known as a hardware interface, where a storage interconnect architecture defines a standard way to communicate and recognize such communications, such as Serial Attached Small Computer System Interface (SCSI) (SAS), Serial Advanced Technology Attachment (SATA), Fibre Channel, etc. These storage interconnect architectures allow a device to maintain one or more connections to another end device via a point-to-point connection, an arbitrated loop of devices, an expander providing a connection to further end devices, or a fabric comprising interconnected switches providing connections to multiple end devices. In the SAS/SATA architecture, a SAS port is comprised of one or more SAS PHYs, where each SAS PHY interfaces a physical layer, i.e., the physical interface or connection, and a SAS link layer having multiple protocol link layer. Communications from the SAS PHYs in a port are processed by the transport layers for that port. There is one transport layer for each SAS port to interface with each type of application layer supported by the port. A "PHY" as defined in the SAS protocol is a device object that is used to interface to other devices and a physical interface. Further details on the SAS architecture for devices and expanders is described in the technology specification "Information Technology--Serial Attached SCSI (SAS)", reference no. ISO/IEC 14776-150:200x and ANSI INCITS.***:200x PHY layer (Jul. 9, 2003), published by ANSI; details on the Fibre Channel architecture are described in the technology specification "Fibre Channel Framing and Signaling Interface", document no. ISO/IEC AWI 14165-25; details on the SATA architecture are described in the technology specification "Serial ATA: High Speed Serialized AT Attachment" Rev. 1.0A (January 2003).

Mitchell et al., as modified by Nadeau et al., discloses a prior art method and system for dynamically reconfiguring pervasive device communication channels; and providing controlled access of requests from virtual private network devices to managed information objects using simple network management protocol upon which the claimed invention can be seen as an improvement.

Seto et al. teaches a prior art comparable system and method of an adaptor supporting different protocols comprising a method of obtaining, by a monitoring device, from a device object associated with a network device, the application layer protocol specific information for accessing the network device using a selected communication application layer protocol.

Thus, the manner of enhancing a particular device (system and method of an adaptor supporting different protocols comprising a method of obtaining, by a monitoring device, from a device object associated with a network device, the application layer protocol specific information for accessing the network device using a selected communication application layer protocol) was made part of the ordinary capabilities of one skilled in the art based upon the teaching of such improvement in Seto et al. Accordingly, one of ordinary skill in the art would have been capable of applying this known improvement technique in the same manner to the prior art method and system for dynamically reconfiguring pervasive device communication channels; and providing controlled access of requests from virtual private network devices to managed information objects using simple network management protocol of Mitchell et al., as modified by Nadeau et al., and the results would have been predictable to one of ordinary skill in the art, namely, one skilled in the art would have readily recognized a method and system of a multi-channel protocol controller.

Consider claims 2, 10 and 17, as applied to claims 1, 9 and 16, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the step of performing further tests comprises: determining whether a vendor of the network device can be obtained from the network device using the selected communication protocol; if the preceding determining step determines that the vendor can not be obtained using the selected communication protocol, checking whether the selected communication protocol supports a generic vendor, and if the selected communication protocol does not support the generic vendor, removing, from the device object, the information for accessing the network device using the selected communication protocol; if the preceding determining step determines that the vendor can be obtained using the selected communication protocol, obtaining the vendor from the network device and determining whether the obtained vendor is supported by the selected communication protocol ((“Consequently, a request associated with one particular VPN cannot obtain information that is associated with another VPN. Further, because MIB object instances associated with a particular VPN provide appropriate access information in the form of a securityName, object instances may be created, deleted or modified on a per-VPN basis, without requiring the instrumentation to determine whether a particular Object Instance resides within a particular VPN. In addition, SNMP Agents and their MIBs can become "VPN aware" without modification to the SNMP Agent code or the MIBs.") Nadeau et al., column 11 lines 45-55); if the obtained vendor is not supported by the selected communication protocol, checking whether the selected communication protocol supports the generic vendor, and if the selected communication protocol does not support the generic vendor, removing, from the device object, the information for accessing the network device using the selected communication protocol; and if the obtained vendor is supported by the selected communication protocol, performing further tests related to model information (("The MIB tree is also extensible by virtue of experimental, proprietary and/or private branches. There are now more of these enterprise-specific proprietary MIB modules, defined unilaterally by various vendors and other groups, than standards-based MIB modules. Consequently, there are now a virtually uncountable number of defined objects.") Nadeau et al., column 9 lines 38-44).

Consider claims 3, 11 and 18, as applied to claims 2, 10 and 17, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the step of performing further tests related to model information comprises: determining whether a model of the network device can be obtained from the network device using the selected communication protocol; if the preceding determining step determines that the model can not be obtained using the selected communication protocol, checking whether the selected communication protocol supports a generic model, and if the selected communication protocol does not support the generic model, removing, from the device object, the information for accessing the network device using the selected communication protocol (Mitchell et al., paragraph 0037); if the preceding determining step determines that the model can be obtained using the selected communication protocol, obtaining the model from the network device and determining whether the obtained model is supported by the selected communication protocol; and if the obtained model is not supported by the selected communication protocol, checking whether the selected communication protocol supports the generic model, and if the selected communication protocol does not support the generic model, removing, from the device object, the information for accessing the network device using the selected communication protocol ((“Although a number of architectures may be used to implement the clients 130, 150, and 170, it may be helpful to describe on useful architecture for providing the functionality described herein. FIG. 3 illustrates one telematics client architecture 300 that is particularly useful for clients 130, 170 that have higher capacity processors and memory available. The illustrated architecture 300 is an OSGi architecture with a J2ME CDC platform but, of course, other container frameworks (such as any Java-based container framework or other object-oriented framework) or other architectures may be utilized for the architecture 300. As with other OSGi architectures, the client architecture 300 is built on an operating system 304 (such as the host operating system for the client 130, 170) upon which drivers 308 and original equipment manufacturer (OEM) specific native code 306 are provided. The client architecture 300 further includes a virtual machine 310, such as a CDC-compliant Java.TM. Virtual Machine (JVM), upon which are built the OSGi framework 312 and OEM-code 314 specific to the virtual machine 310.") Mitchell et al., paragraph 0033).

Consider claims 4, 12 and 19, as applied to claims 1, 9 and 16, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the obtaining step comprises: obtaining, from the device object, a protocol parameter map comprising at least one entry, wherein each entry comprises a protocol string and a corresponding vector of information used to access the network device using a protocol indicated in the protocol string (("In block 620, the securityName is looked up in the VAC MIB Table, and in block 622 a determination is made whether the securityName is found in the lookup operation. If the specified context string is found in the table of MIB Views, then the test of block 622 is affirmative, and control passes to block 624. In general, in succeeding steps, the access control policy for that context string is accessed in the form of MIB Views that correspond to the protocol operation in the request.") Nadeau et al., column 16 lines 37-45).

Consider claims 5, 13 and 20, as applied to claims 1, 9 and 16, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the step of determining if the network device can be accessed comprises: transmitting, to the network device, the information for accessing the network device using the selected communication protocol (("The read-view 508 represents the set of Object Instances to which a group is authorized to access when reading objects. Reading objects occurs when processing a retrieval operation, i.e., when handling Read Class PDUs. The write-view 510 represents the set of Object Instances authorized for the group when writing objects. Writing objects occurs when processing a write operation, i.e., when handling Write Class PDUs. The notify-view 512 represents the set of Object Instances authorized for the group when sending objects in a notification, such as when sending a notification, i.e., when sending Notification Class PDUs.") Nadeau et al., column 13 lines 34-44); receiving, by the network device, the transmitted information (Mitchell et al., paragraph 0023); and determining if the network device responds to the received information indicating that the network device can be accessed using the selected communication protocol (Mitchell et al., paragraph 0032).

Consider claims 7, 14 and 22, as applied to claims 1, 9 and 16, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the selecting step comprises: selecting the communication protocol among SNMP, HTTP, and FTP (("In the following discussion, computer and network devices, such as the software and hardware devices within the mobile client 130, the light mobile client 150, the non-mobile client 170, the on-board communications system 200, and the service providers 110, are described in relation to their function rather than as being limited to particular electronic devices and computer architectures. To practice the invention, the computer and network devices may be any devices useful for providing the described functions, including well-known data processing and communication devices and systems such as portions of in-vehicle computer systems, personal digital assistants, personal, laptop, and notebook computers and mobile computing devices with processing, memory, and input/output components, and server devices configured to maintain and then transmit digital data over a communications network. Similarly, the wired and wireless client devices may be any electronic or computing device for transmitting digital data over a wired or wireless network and are typically installed or resident within mobile vehicles such as automobiles, airplanes, ships, mobile computers and computing devices, and the like or in stationary structures such as residential structures or buildings utilized by businesses. Data, including client requests, service provider or carrier and content provider requests and responses, and transmissions to and from the clients 130, 150, 170 and among other components of the system 100 typically is communicated in digital format following standard communication and transfer protocols, such as TCP/IP, HTTP, HTTPS, FTP, IMAP and the like, or IP or non-IP wireless communication protocols such as TCP/IP, TL/PDC-P, WSP, Bluetooth, 802.11b, and the like, but this is not intended as a limitation of the invention. Additionally, the invention is directed toward provisioning of communication filter and protocol elements and the dynamic creation of communication channels for applications on clients 130, 150, 170, but is not limited to a specific native language within the client devices (although Java.TM. language implementations are provided for the sake of simplicity and to provide at least on specific example), a particular function of an application, or a specific client configuration.") Mitchell et al., paragraph 0021).

Consider claims 8, 15 and 23, as applied to claims 1, 9 and 16, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the step of performing further tests comprises: checking whether the selected communication protocol is SNMP, wherein, if the checking step determines that the selected communication protocol is SNMP, the selected communication protocol can be used to extract the status information from the network device ((“In one embodiment, a function located in existing SNMP Agent code is adapted to provide a new access control function. Specifically, a FindFirst( ) function is used. In conventional SNMP implementations, the FindFirst( ) function is generated as a "stub" function and is later modified by the user to find an appropriate table pointer. This pointer is then passed to other operations that use it in addition to the managed object instance ID, which serves as an index to find a specific object in memory. Accordingly, as indicated in block 634, using the FindFirst( ) function, the process queries or modifies objects or functions in the IOS software to locate appropriate variable values for processing, or to modify a specified object, and to return a status value. According to an embodiment, the FindFirst( ) function is modified to provide two processing paths based on whether a VPN ID is provided in the function call. At block 636, a test is carried out to determine whether a VPN ID is specified in the form of a securityName value in the request.”) Nadeau et al., column 17 lines 22-40).

Consider claims 24, 25 and 26, as applied to claims 1, 9 and 16, respectively. Mitchell et al., as modified by Nadeau et al. and Seto et al., discloses a system and method wherein the step of determining if the network device can be accessed comprises: determining if the network device can be accessed by a monitoring computer using the selected communication protocol and the information for accessing the network device obtained from the device object ((“More particularly, the service provider 110 stores (or has access to) available services or software applications 112, available communication filters 114, and available protocol elements 116. As will become clear, communication channels built within the clients 130, 150, 170 and used by client applications or service components 140, 154, 180 are formed generally by the combination of a single protocol element, such as element 116, that defines network protocols and one or more communication filters, such as a filter(s) 114 that define communication parameters (such as what security measures are to be taken and how to apply such measures). A provisioning agent 118 is provided on the service provider 110 to control which services 112, filters 114, and protocol elements 116 are made available which clients 130, 150, and 170. The provisioning agent 118 responds to discovery requests from the clients 130, 150, 170 and when appropriate transfers or provisions the services 112, filters 114, and protocol elements 116 to the clients 130, 150, 170. The filters 114 and protocol elements 116 may be provided by the content providers 104 or another third-party and typically are registered within the service provider 110 (such as in a filter and protocol element registry) and then announced or pushed (or otherwise made available) to the clients 130, 150, 170. Once the filter 114 and/or network protocol element 116 has been deployed to the client 130, 150, 170 the client 130, 150, 170 may begin to use the filters 114 and elements 116 in forming or reconfiguring service component communication channels, as explained below in detail. The service provider 110 may further, such as with the provisioning agent 118, maintain a database (not shown) with information about which filters 114 and which protocol elements 116 have been deployed to which clients 130, 150, 170.") Mitchell et al., paragraph 0023 ("A method as recited in claim 1, further comprising the steps of providing, at the managed network device, the second mapping, and wherein the steps of identifying a subset of objects and providing access comprise the steps of: determining whether the securityName value from the request is in the second mapping; when the securityName value from the request is in the second mapping: identifying a management information base variable referenced in the request; based on one or more views referenced in the second mapping, determining whether a protocol operation of the request is allowed for the variable; dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.") Nadeau et al., Claim 4)

### ***Response to Arguments***

**7.** Applicant's arguments filed 17 August 2009 with respect to claims 1, 9, and 16 have been considered but are moot in view of the new ground(s) of rejection.

### *Conclusion*

**8.** Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any response to this Office Action should be faxed to (571) 273-8300 or mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

**Customer Service Window**
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Mark Fearer whose telephone number is (571) 270-1770. The Examiner can normally be reached on Monday-Thursday from 7:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Tonia Dollinger can be reached on (571) 272-4170. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Mark Fearer
/M.D.F./
December 1, 2009

/George C Neurauter, Jr./
Primary Examiner, Art Unit 2443